IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

STEVEN GREEK and JON BOYAJIAN, individually and on behalf of all others similarly situated, Plaintiffs, v. 90 DEGREE BENEFITS, INC. and 90 DEGREE BENEFITS, LLC, Defendants.	Case No. 23-cv-511 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Steven Greek and Jon Boyajian ("Plaintiffs"), individually and on behalf of all others similarly situated, through Counsel, and for the Class Action Complaint against Defendants 90 Degree Benefits, Inc. and 90 Degree Benefits, LLC (collectively, "Defendants" or "90 Degree Benefits"), and alleges upon personal knowledge as to their own actions and experiences, and upon investigation, information, and belief as to all other matters, as follows:

INTRODUCTION

1. This consumer data breach lawsuit arises out of Defendants' failure to implement and maintain adequate security and safeguards with respect to the collection and maintenance of highly sensitive and confidential personal information of their customers, including Plaintiffs' and Class members' names, Social Security numbers, addresses, dates of birth, medical/health information, and payment information. Defendants' insufficient and unreasonable data security practices caused, facilitated, and exacerbated the data breach and its impact on Plaintiffs and Class members.

2. 90 Degree Benefits is a health insurance company that designs health plans and administers benefits for employers' health and operational needs.[1]

3. On or around April 7, 2023, Defendants sent to Plaintiffs and Class members a letter entitled "Notice of Data Security Incident" ("Notice"). The Notice stated that, between December 5, 2022 and December 11, 2022, an unauthorized actor had the ability to access certain information stored on Defendants' network (the "Data Breach"). According to Defendants, on or about December 10, 2022, Defendants identified suspicious activity on its network. Through a subsequent forensic investigation, it was determined that certain systems and files containing personal information of their customers were accessed without authorization. Although Defendants identified suspicious activity much earlier, Defendants did not warn those most at risk––Plaintiffs and Class members—until April 7, 2023.

4. The Data Breach exposed Plaintiffs' and Class members' personally identifiable information to criminals, including, but not limited to, their names, Social Security numbers, addresses, dates of birth, medical/health information, and payment information. All of the foregoing information pertaining to Plaintiffs and Class members constitutes "personally identifiable information" as well as "protected health information" and is referred to herein as "PII and PHI."

5. The PII and PHI that Defendants failed to protect with reasonable safeguards can be used by criminals alone, and in conjunction with other pieces of information, to perpetrate crimes against Plaintiffs and Class members that can result in significant liability and damage to their money, property, creditworthiness, reputation, and their ability to prove their identity, pay current loans, improve their credit, and/or obtain loans on favorable terms in the future.

[1] https://90degreebenefits.com/about.php (last visited April 19, 2023).

6. Plaintiffs and Class members entrusted Defendants with their PII and PHI. Defendants understand the importance of protecting such information. For example, on one of Defendants' websites, it states: "We recognize and respect your desire for privacy when it comes to your personal and health care affairs" and explains that "We maintain this information, as well as all web based transactions, according to our usual high, government regulated, security and confidentiality standards."[2]

7. Defendants' representations concerning privacy practices and data security were false. In December 2022, criminals breached Defendants' inadequately defended systems, and accessed and acquired electronic files containing the PII and PHI of 181,543 Class members. The criminals gained unauthorized access by thwarting, circumventing, and defeating Defendants' unreasonably deficient data security measures and protocols. In fact, this is not Defendants' first major data breach. Less than a year earlier, in February 2022, Defendants experienced a similar but different data breach.[3] Accordingly, Defendants were on direct notice of the need to implement advanced data security protections but clearly failed to do so.

8. Plaintiffs, individually, and on behalf of all persons similarly situated, seek to be made whole for the losses incurred as a result of the Data Breach, and the losses that will be incurred in the future. Plaintiffs also seek injunctive relief in the form of compliant data security practices, full disclosure regarding the disposition of the information in Defendants' systems, and monitoring and audits of Defendants' security practices going forward because Defendants continue to collect, maintain, and store Plaintiffs' and Class members' PII and PHI. Due to the sensitive and immutable nature of the PII and PHI at issue, especially Social Security numbers and

[2] *See* https://90degreebenefits.com/privacy.php (last visited April 19, 2023).
[3] *See* https://oag.ca.gov/system/files/90%20Degree%20Benefits%20-%20Sample%20Notice.pdf.

medical information, Plaintiffs and Class members will need to, among other things, enroll is identity theft protective services for their respective lifetimes.

PARTIES, JURISDICTION, AND VENUE

9. Plaintiff Steven Greek ("Plaintiff Greek") is a resident and citizen of the State of Texas. Plaintiff Greek received a letter from 90 Degree Benefits, notifying him that his PII and PHI, including his Social Security number and medical information, had been compromised in the Data Breach.

10. Plaintiff Jon Boyajian ("Plaintiff Boyajian") is a resident and citizen of the State of Ohio. Plaintiff Boyajian received a letter from 90 Degree Benefits, notifying him that his PII and PHI, including his Social Security number and medical information, had been compromised in the Data Breach.

11. Defendant 90 Degree Benefits, Inc., formerly known as EBSO, Inc., has its principal place of business in the City of Glendale, Milwaukee County, Wisconsin. Upon information and belief, 90 Degree Benefits, Inc. merged with 90 Degree Benefits, LLC in or around December 2018. 90 Degree Benefits, Inc. is a Wisconsin regional office of 90 Degree Benefits, LLC.

12. Defendant 90 Degree Benefits, LLC is a limited liability company with its principal place of business in Birmingham, Alabama.

13. The Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action involving 100 or more Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Many members of the Class, including Plaintiffs, are citizens of different states from Defendants.

14. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2), as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendants conducts substantial business in this District.

15. All of Plaintiffs' and Class Members' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns. As the corporate relationship between the two Defendants and other possible defendants is not fully known, Plaintiffs and Class Members reserve the right to amend the complaint should the facts and the evidence necessitate it.

GENERAL ALLEGATIONS

Background

16. For 90 Degree Benefits to perform their health benefits services, from which they generate their profits, Defendants collect and store the PII and PHI of individuals, including Plaintiffs and the Class.

17. Due to the highly sensitive and personal nature of the information Defendants acquire and store with respect to health insurance customers, Defendants recognize the privacy rights of the individuals whose PII and PHI Defendants obtains, as evidenced by 90 Degree Benefits' publicly available privacy policy ("Privacy Notice").[4]

18. Plaintiffs and the Class Members reasonably expected that Defendants would implement and maintain reasonable data security measures to protect their PII and PHI from foreseeable threats.

19. Plaintiffs and Class Members relied on these sophisticated Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes

[4] https://90degreebenefits.com/privacy.php (last visited April 19, 2023).

only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their sensitive PII and PHI.

20. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII and PHI from involuntary disclosure to third parties.

The Data Breach

21. According to Defendants, on or about December 10, 2022, Defendants identified suspicious activity on their network. Through a subsequent forensic investigation, it was determined that certain systems and files containing personal information of Defendants' customers were accessed without authorization between December 5, 2022 and December 11, 2022. Although Defendants identified suspicious activity much earlier, Defendants did not warn those most at risk—Plaintiffs and Class members—until April 7, 2023, via mailed Notice.

22. The Notice states that Plaintiffs' and Class members' PII and PHI was accessed by an unauthorized person in the Data Breach.

23. The Notice states that Plaintiffs' and Class members' PII and PHI accessed in the Data Breach includes their names, Social Security numbers, addresses, dates of birth, medical/health information, and payment information.

24. Due to Defendants' inadequate and insufficient data security measures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft and must live with that threat forever. Plaintiffs believe their PII and PHI was both stolen in the Data Breach and is still in the hands of the cybercriminal "hackers." Plaintiffs further believe their PII and PHI was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals who perpetrate cyberattacks of the type that occurred here.

90 Degree Benefits are HIPAA Covered Entities

25. Defendants are HIPAA covered business associates that provide services to various health care providers (*i.e.*, HIPAA "Covered Entities"). As a regular and necessary part of their business, Defendants collect and maintain the highly sensitive PII of their clients' patients and health plan Members. Defendants are required under federal and state law to maintain the strictest confidentiality of the patient's and plan Members' PII and PHI that they require, receive, and collect. Defendants are further required to maintain sufficient safeguards to protect that PII and PHI from being accessed by unauthorized third parties.

26. As HIPAA covered business entities, Defendants are required to enter into contracts with their Covered Entities to ensure that they will implement adequate safeguards to prevent unauthorized use or disclosure of PII and PHI, including by implementing requirements of the HIPAA Security Rule,[5] and to report to the Covered Entities any unauthorized use or disclosure of PII and PHI, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

27. As a condition of receiving Defendants' services, Defendants require that Covered Entities and their patients and plan Members, including Plaintiffs and Class Members, entrust them with highly sensitive personal information. Due to the nature of Defendants' business, which includes providing brand management, local marketing, marketing execution, print production and supply chain logistics, Defendants would be unable to engage in their regular business

[5] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

activities without collecting and aggregating PII and PHI that they know and understand to be sensitive and confidential.

28. Plaintiffs and Class Members are, or were, patients whose medical records were maintained by, or who received health-related or other services from, Defendants through their healthcare provider customers, and who directly or indirectly entrusted Defendants with their PII and PHI. Plaintiffs and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PII and PHI confidential.

Industry Standards for Data Security

29. Defendants are aware of the importance of safeguarding Plaintiffs' and Class members' PII and PHI, and that by virtue of their business, they owe duties to Plaintiffs and Class members to take reasonable measures to safeguard PII and PHI that foreseeably is targeted by criminals.

30. Defendants are aware that the PII and PHI that they collect, organize, and store, can be used by criminals to engage in crimes such as identity fraud and theft using Plaintiffs' and Class members' PII and PHI.

31. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the financial industry preceding the date of the breach.

32. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[6]

[6] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at: https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/), at 6 (last visited on Feb. 4, 2023).

33. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers … Many of them were caused by flaws in ... systems either online or in stores."[7]

34. This is particularly true for healthcare providers. Experts studying cybersecurity routinely identify healthcare providers and their business associates as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

35. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[8]

36. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[9]

---

[7] Dennis Green, Mary Hanbury & Aine Cain, If you bought anything from these 19 companies recently, your data may have been stolen, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited Feb. 4, 2023).

[8] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Aug. 2, 2022).

[9] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited October 5, 2022).

37. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[10]

38. In light of this and recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), 90 Degree Benefits knew or should have known that their electronic records would be targeted by cybercriminals.

39. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the Defendant's industry, including Defendants.

40. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities … are attractive to ransomware criminals … because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[11]

[10] *Cost of a Data Breach Report 2022*, IBM Security, available: https://www.ibm.com/downloads/cas/3R8N1DZJ.

[11] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), available at: https://www.law360.com/articles/1220974/fbi- secret-service-warn-of-targeted-ransomware (last visited Feb. , 2023).

41. Moreover, PII and PHI are valuable property.[12] "Firms are now able to attain significant within the existing legal and regulatory frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII and PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

42. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII and PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

43. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.[15]

---

[12] *See* Marc van Lieshout, The Value of Personal Data, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data. (last visited Feb. 4, 2023).

[13] OECD, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited Feb. 4, 2023).

[14] IAB Data Center of Excellence, U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited Feb. 4, 2023).

[15] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011)

44. Because of Defendants' failure to implement, maintain, and comply with necessary cybersecurity requirements, Defendants were unable to protect Plaintiffs' and Class members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality. As a proximate result of such failures, criminals gained unauthorized access to Defendants' systems, and acquired Plaintiffs' and Class members' PII and PHI in the Data Breach without being stopped.

45. Defendants were unable to prevent the Data Breach, and were unable to detect the unauthorized access to vast quantities of sensitive and protected files containing protected information of Plaintiffs and Class members. Discovery on Defendants, law enforcement investigators, and private investigators, will reveal more specific facts about Defendants' deficient and unreasonable security procedures.

46. Security standards commonly accepted among businesses that store personal information using the Internet include, without limitation:

a) Maintaining a secure firewall configuration;

b) Monitoring for suspicious or irregular traffic to servers;

c) Monitoring for suspicious credentials used to access servers;

d) Monitoring for suspicious or irregular activity by known users;

e) Monitoring for suspicious or unknown users;

f) Monitoring for suspicious or irregular server requests;

g) Monitoring for server requests for personal information;

h) Monitoring for server requests from Virtual Private Networks ("VPNs"); and

https://www.jstor.org/stable/23015560?seq=1 (last visited Feb. 4, 2023).

i) Monitoring for server requests from Tor exit nodes.

47. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[16] and protection of personal information[17] which includes basic security standards applicable to all types of businesses.

48. The FTC recommends that businesses:

a) Identify all connections to the computers where you store sensitive information;

b) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c) Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d) Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e) Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f) Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g) Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides

[16] *See* F.T.C., *Start with Security: A Guide for Business*, (June 2015), https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last accessed Feb. 8, 2023).

[17] *See* F.T.C., *Protecting Personal Information: A Guide for Business*, (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Feb. 8, 2023).

is only as effective as its access controls, they should be reviewed periodically;

h) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

49. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[18]

50. Several best practices have been identified that at a minimum should be implemented by HIPAA covered business entities like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

51. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such

[18] F.T.C., *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

as firewalls, switches, and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points.

52. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

53. These foregoing frameworks are existing and applicable industry standards in the healthcare industry. Defendants failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

54. Because Defendants were entrusted with consumers' PII and PHI, they have a duty to keep the PII and PHI secure.

55. Plaintiffs and Class members reasonably expect that when they provide their PII and PHI to a company, the company will take reasonable measures to safeguard their PII and PHI from foreseeable cyberattacks.

56. Despite Defendants' obligations, Defendants failed to upgrade and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

57. Specifically, in breach of their duties, Defendants failed to:

a) Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;

b) Block all inbound and outbound Internet, email, and network traffic to foreign countries;

c) Maintain a secure firewall configuration;

d) Monitor for suspicious or irregular traffic to servers;

e) Monitor for suspicious credentials used to access servers;

f) Monitor for suspicious or irregular activity by known users;

g) Monitor for suspicious or unknown users;

h) Monitor for suspicious or irregular server requests;

i) Monitor for server requests for personal and financial information;

j) Monitor for server requests from VPNs;

k) Monitor for server requests from Tor exit nodes;

l) Identify all connections to the computers where Defendants store sensitive information;

m) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

n) Scan computers on Defendants' network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;

o) Pay particular attention to the security of Defendants' web applications—the software used to give information to visitors to their websites and to retrieve information from them;

p) Use a firewall to protect Defendants' computers from hacker attacks while they are connected to a network, especially the Internet;

q) Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

r) Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

s) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

t) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

58. Had Defendants properly maintained their systems and adequately protected them, Defendants could have prevented the Data Breach.

59. As HIPAA covered business associates, Defendants should have known about their data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the PII and PHI stored in its unprotected files and *given that Defendants experienced a large data breach just months before*.[19]

Defendants Owed Duties to Plaintiffs and Class Members to Adequately Secure and Safeguard Their PII and PHI

60. Defendants are aware of the importance of security in maintaining personal information (particularly sensitive personal information), and the value consumers place on keeping their PII and PHI secure.

61. Defendants owe duties to Plaintiffs and Class members to maintain adequate security and safeguards to protect the confidentiality of their PII and PHI.

62. Defendants owe further duties to customers to immediately and accurately notify them of a breach of their systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

[19] https://oag.ca.gov/system/files/90%20Degree%20Benefits%20-%20Sample%20Notice.pdf.

The Categories of PII and PHI at Issue Here Are Valuable to Criminals

63. Businesses that solicit, aggregate, and store sensitive PII and PHI are likely to be targeted by cyber criminals.

64. The FTC has released its updated publication on protecting PII and PHI for businesses, which includes instructions on protecting PII and PHI, properly disposing of PII and PHI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

65. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect PII and PHI. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII and PHI as a violation of the FTC Act, 15 U.S.C. § 45.

66. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to a U.S. Government Accountability Office report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

67. Companies recognize that PII and PHI is a valuable asset. Indeed, PII and PHI is a valuable commodity. A "cyber black-market" exists in which criminals openly post PII and PHI on a number of Internet websites. Plaintiffs' and Class members' personal data that was stolen has a high value on both legitimate and black markets.

[20] *See* https://www.gao.gov/assets/gao-07-737.pdf at 29 (last accessed Feb. 4, 2023).

68. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[21]

69. Individuals rightfully place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy—and the amount is considerable.

70. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information—the very injury at issue here—between $11.33 and $16.58 per website.[22] The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49 – 44.62."[23] This study was done in 2002. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII and PHI to bad actors—would be exponentially higher today.

71. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

---

[21] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, transcript, p. 8, *available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last accessed Feb. 4, 2023).
[22] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at p. 17, Oct. 2002, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last accessed Feb. 8, 2023).
[23] *Id.*

72. To date, Defendants have only offered Plaintiffs and Class members 12 months of identity theft protection. However, this is insufficient considering the fact that Plaintiffs' and Class members' PII and PHI will be used by identity thieves for many years to come.

73. The information Defendants allowed to be compromised and taken is of such a nature that the harms to Plaintiffs and the Class will continue to grow, and Plaintiffs and Class members will continue to be at substantial risk for further imminent and future harm.

Damages from Data Breaches

74. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.

75. Consumers place a high value not only on their personal information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

76. The United States Government Accountability Office explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1024 (9th Cir. 2018). The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

77. The FTC recommends that identity theft victims take several steps to protect their personal information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports often, contacting companies to remove fraudulent charges from their

accounts, placing a credit freeze (which restricts creditors' access to the victim's credit reports, effectively preventing creditors from approving new extensions of credit), and correcting their credit reports.

78. Identity thieves use stolen personal information for "various types of criminal activities, such as when PII is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank fraud and government fraud." *In re Zappos.com, Inc.*, 888 F.3d at 1024. The information exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are ways for hackers to exploit information they already have to get even more personally identifying information through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

79. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

80. Personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

81. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, or are yet to be dumped on the black market, meaning Plaintiffs

[24] *See* GAO Report, at p. 29.

and Class members are at an increased risk of fraud and identity theft for many years into the future. This is why Defendants' one-year credit monitoring offering is inadequate.

82. Data breaches are preventable. As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised ...."

83. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures.... Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

84. Here, Defendants presumably took actions to secure the affected systems *after* the Data Breach at issue in this action, but should have implemented those actions previously to *prevent* the Data Breach. This is undeniably true in light of the large-scale data breach that affected Defendants *just months before*.

85. The types of information Defendants acknowledge were stolen by the criminals are sufficiently sensitive and valuable to identity thieves and criminals in perpetrating identity crimes. This information can be used to perpetrate scams, victimize the persons who own the information, and commit identity theft and fraud.

86. Criminals can use PII and PHI to devise and employ phishing and social engineering schemes capitalizing on the genuine information stolen from Defendants to send fraudulent mail and other communications to Plaintiffs and Class members that look authentic, but

which are designed to lure them into paying money or providing other information that the criminals can use to steal money.

87. For instance, with a stolen Social Security number, which is only one category of the PII and PHI compromised in the Data Breach, someone can open financial accounts, file fraudulent tax returns, commit crimes, and steal benefits.[25]

88. Victims of the Data Breach, like Plaintiffs and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[26]

89. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other information for unauthorized activity for years to come.

90. Plaintiffs and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII and PHI;

[25] *See, e.g.*, Christine DiGangi, 5 Ways an Identity Thief Can Use Your Social Security Number, Nov. 2, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/ (last visited Feb. 4, 2023).
[26] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last visited Feb. 4, 2023).

b. Improper disclosure of their PII and PHI;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII and PHI being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential information used against them by spam callers to defraud them;

e. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of individuals' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII and PHI; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

91. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII and PHI, which remains in the possession of Defendants, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily

compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiffs' and Class members' PII and PHI.

92. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendants has caused them but, given the kind of PII and PHI Defendants made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PII and PHI, Plaintiffs and Class members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[27]

Defendants Could Have Prevented the Breach but Failed to Adequately Protect the PII and PHI of the Plaintiffs and Class Members

93. Data disclosures and data breaches are preventable.[28] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[29] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised ... ."[30]

94. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures ... Appropriate information

[27] Will a New Social Security Number Affect Your Credit?, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html#:~:text=Will%20a%20new%20Social%20Security,when%20determining%20someone's%20credit%20score. (last visited Feb. 4, 2023).
[28] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[29] *Id.*
[30] *Id.*

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[31]

95. Defendants obtained and stored Plaintiffs' and Class members' PII and PHI—including but not limited to, their names and Social Security numbers—and were entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII and PHI.

96. Defendants breached fiduciary duties owed to Plaintiffs and the Class as guardians of their PII and PHI.

97. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendants' failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiffs' and Class members' PII and PHI.

98. Defendants maintained the PII and PHI in an objectively reckless manner, making the PII and PHI vulnerable to unauthorized disclosure.

99. Defendants knew, or reasonably should have known, of the importance of safeguarding PII and PHI and of the foreseeable consequences that would occur if Plaintiffs' and Class members' PII and PHI was stolen, including the significant costs that would be placed on Plaintiffs and Class members as a result of a breach.

100. The risk of improper disclosure of Plaintiffs' and Class members' PII and PHI was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure Plaintiffs' and Class members' PII and PHI from that risk left the PII and PHI in a dangerous condition.

[31] *Id.*

101. Defendants disregarded the rights of Plaintiffs and Class members by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the PII and PHI was protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PII and PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

Facts Related to Plaintiff Greek

102. Plaintiff Greek received a letter from 90 Degree Benefits in April 2023, advising him that his PII and PHI – including his name, Social Security number, address, date of birth, medical/health information, and payment information – was accessed or acquired by cybercriminals in the Data Breach.

103. As a result of Defendants' negligence and failure to properly secure the PII and PHI in their possession, which negligence and failure led to the Data Breach, Plaintiff Greek's PII and PHI has been obtained by cybercriminals.

104. Plaintiff Greek is now under a present an imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Greek's life. The imminent risk of identity theft and fraud Plaintiff Greek now faces is substantial, certainly impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

105. As a result of the Data Breach, Plaintiff Greek has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and

address the future consequences of the Data Breach for Plaintiff Greek, including (but not limited to) investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, reviewing accounts statements, and monitoring other personal information.

106. As a direct and proximate result of the Data Breach, Plaintiff Greek will need to have identity theft protection for the foreseeable future.

107. Plaintiff Greek has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Greek's PII and PHI. Additionally, Plaintiff Greek's PII and PHI is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Facts Related to Plaintiff Boyajian

108. Plaintiff Boyajian received a letter from 90 Degree Benefits in April 2023, advising him that his PII and PHI – including his name, Social Security number, address, date of birth, medical/health information, and payment information – was accessed or acquired by cybercriminals in the Data Breach.

109. As a result of Defendants' negligence and failure to properly secure the PII and PHI in their possession, which negligence and failure led to the Data Breach, Plaintiff Boyajian's PII and PHI has been obtained by cybercriminals.

110. Plaintiff Boyajian is now under a present and imminent risk of subsequent identity theft and fraud and will remain under such risk for the rest of Plaintiff Boyajian's life. The imminent risk of identity theft and fraud Plaintiff Boyajian now faces is substantial, certainly

impending, continuous, and ongoing because of the negligence of Defendants in their failure to implement adequate data security protocols, which negligence led to the Data Breach.

111. As a result of the Data Breach, Plaintiff Boyajian has also expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach for Plaintiff Boyajian, including (but not limited to) investigating the Data Breach, investigating how best to protect his information from further identity theft, and monitoring his personal information.

112. As a direct and proximate result of the Data Breach, Plaintiff Boyajian will need to have identity theft protection for the foreseeable future.

113. Plaintiff Boyajian has suffered additional injury directly and proximately caused by the Data Breach, including damages and diminution in the value of Plaintiff Boyajian's PII and PHI. Additionally, Plaintiff Boyajian's PII and PHI is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to future wrongful disclosures and/or security breaches so long as Defendants fails to undertake appropriate and adequate measures, including the implementation of enhanced employee training and data security protocols, to protect it.

Plaintiffs' and Class Members' Damages

140. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

141. Plaintiffs and Class members have or will suffer actual injury as a direct result of the Data Breach including:

a) Spending time reviewing charges for any fraudulent charges and remedying any fraudulent charges found;

b) Purchasing credit monitoring and identity theft prevention;

c) Requesting and reviewing their credit reports;

d) Spending time and money addressing and remedying identity theft;

e) Spending time placing "freezes" and "alerts" with credit reporting agencies and, subsequently, temporarily lifting a security freeze on a credit report, or removing a security freeze from a credit report;

f) Spending time on the phone with, or visiting, financial institutions to dispute fraudulent charges;

g) Contacting their financial institutions and closing or modifying financial accounts compromised as a result of the Data Breach; and

h) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

142. Moreover, Plaintiffs and Class members have an interest in ensuring that their personal information is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data containing their personal information is secure.

143. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy.

144. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members are at an increased and immediate risk of future harm, including from identity theft and fraud.

145. As a result of the Data Breach, Plaintiffs and Class members are at an imminent risk of identity theft and fraud. This risk will continue to exist for years to come, as Plaintiffs and Class members must spend their time being extra vigilant, due to Defendants' failures, to try to prevent being victimized for the rest of their lives.

146. Because Defendants presented such an easy target to cyber criminals, Plaintiffs and Class members have already been subjected to violations of their privacy and have been exposed

to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now and in the future, spend time to more closely monitor their affected PII and PHI to guard against identity theft and other fraud.

147. Plaintiffs and Class members may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services or other protective measures to deter and detect identity theft.

CLASS ACTION ALLEGATIONS

148. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5) on behalf of a class of similarly situated individuals (the "Class") defined as follows:

> All persons residing in the United States whose PII or PHI was accessed or acquired as a result of the 90 Degree Benefits data breach that is the subject of the notice of Data Breach that Defendants sent to Plaintiffs and other Class Members (the "Class").

149. Excluded from the Class are Defendants; any entity in which either Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by either Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families.

150. Plaintiffs reserve the right to modify and/or amend the Class definition, including but not limited to creating subclasses, as necessary.

151. ***Numerosity***. The Class members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class members are unknown at this time, public news reports indicate that approximately 181,543 individuals had their PII and PHI compromised in this Data Breach. The identities of Class members are ascertainable through

Defendants' records, Class members' records, publication notice, self-identification, and other means.

152. ***Commonality***. There are numerous questions of law and fact common to Plaintiffs and Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the PII and PHI of Plaintiffs and Class members;

b. Whether Defendants had a duty not to disclose the PII and PHI of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendants had a duty not to use the PII and PHI of Plaintiffs and Class members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiffs and Class members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class members that their PII and PHI had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class members that their PII and PHI had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class members are entitled to actual damages, nominal damages, treble damages, and/or exemplary damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

153. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class members because Plaintiffs, like all Class members, had his PII and PHI compromised, breached and stolen in the Data Breach. Plaintiffs and Class members were injured through Defendants' uniform misconduct described in this Complaint and assert the same claims for relief.

154. ***Adequacy***. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel who are experienced in class actions and complex litigation, including data privacy litigation of this kind. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

155. ***Predominance***. The questions of law and fact common to Class members predominate over any questions which may affect only individual members.

156. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class members have been harmed by Defendants' wrongful conduct and/or action.

157. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct and/or inaction. No difficulties would be encountered in this litigation that would preclude its maintenance as a class action.

158. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual

members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

159. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2), because Defendants have acted or refused to act on grounds that apply generally to the Class so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Plaintiffs and the Class)

160. Plaintiffs repeat and reallege the forgoing allegations with the same force and effect as though fully set forth herein.

161. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

162. Defendants had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class members' PII and PHI.

163. Defendants had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class members could and would suffer if the data were wrongfully disclosed.

164. Defendants' actions and inactions were of the type that would result in foreseeable, unreasonable risk of harm to Plaintiffs and Class members. Defendants knew, or should have known, of the risks inherent in collecting and storing the personal information of Plaintiffs and Class members and the importance of adequate security in storing the information. Additionally,

Defendants are aware of numerous, well-publicized data breaches that exposed the personal information of individuals.

165. Defendants had a common law duty to prevent foreseeable harm to Plaintiffs' and Class members' PII and PHI. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of the failure of Defendants to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and Class members' personal information would not be unsecured and accessible by unauthorized persons.

166. Defendants had a special relationship with Plaintiffs and Class members. Defendants were entrusted with Plaintiffs' and Class members' personal information, and Defendants were in a position to protect the personal information from unauthorized access.

167. The duties of Defendants also arose under section 5 of the FTC Act, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal information by companies. Various FTC publications, HIPAA publications, and data security breach orders further form the basis of the duties of Defendants.

168. Defendants had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' personal information in their possession so that the PII and PHI would not come within the possession, access, or control of unauthorized persons.

169. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiffs and Class members, the critical

importance of providing adequate security of that data, and the necessity for encrypting all data stored on Defendants' systems.

170. More specifically, the duties of Defendants included, among other things, the following duties, and Defendants carelessly and negligently acted or failed to act in one or more of the following ways:

a. Failing to conduct proper and reasonable due diligence over their data security systems, practices, and procedures;

b. Failing to adopt, implement, and maintain adequate security measures for protecting an individual's personal information to ensure that the information is not accessible online by unauthorized persons;

c. Failing to adopt, implement, and maintain adequate security measures for deleting or destroying personal information when Defendants' business needs no longer required such information to be stored and maintained; and

d. Failing to adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches, and notify affected persons without unreasonable delay.

171. Defendants breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting personal information in their possession so that the information would not come within the possession, access, or control of unauthorized persons.

172. Defendants acted with reckless disregard for the security of the personal information of Plaintiffs and Class members because Defendants knew or should have known that their data security was not adequate to safeguard the personal information that was collected and stored.

173. Defendants acted with reckless disregard for the rights of Plaintiffs and Class members by failing to promptly detect the Data Breach, and further, by failing to notify Plaintiffs and Class members of the Data Breach in the most expedient time possible and without

unreasonable delay pursuant to common law duties to provide reasonably timely and truthful data-breach notification, so that Plaintiffs and Class members could promptly take measures to protect themselves from the consequences of the unauthorized access to the personal information compromised in the Data Breach.

174. As a result of the unlawful conduct of Defendants, Plaintiffs and Class members have suffered and will continue to suffer foreseeable harm, including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

175. Plaintiffs repeat and reallege the foregoing allegations with the same force and effect as though fully set forth herein.

176. In connection with the dealings Plaintiffs and Class members had with 90 Degree Benefits, Plaintiffs and Class members entered into implied contracts with 90 Degree Benefits.

177. Pursuant to these implied contracts, Plaintiffs and Class members provided 90 Degree Benefits with their PII and PHI in order for 90 Degree Benefits to provide health insurance and benefit services. In exchange, 90 Degree Benefits agreed to, among other things, and Plaintiffs and Class members understood that 90 Degree Benefits would: (1) provide services to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of

Plaintiffs' and Class members' PII and PHI; and (3) protect Plaintiffs' and Class members PII and PHI in compliance with federal and state laws and regulations and industry standards.

178. The protection of PII and PHI was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and 90 Degree Benefits, on the other hand. Indeed, 90 Degree Benefits was clear in its Privacy Policy, and Plaintiff understood that 90 Degree Benefits supposedly respects and is committed to protecting customer privacy.

179. Had the Plaintiffs and Class members known that 90 Degree Benefits would not adequately protect its clients' customers' and former customers' PII and PHI, they would not have provided 90 Degree Benefits or 90 Degree Benefits' clients with their PII and PHI.

180. Plaintiffs and Class members performed their obligations under the implied contracts when they provided 90 Degree Benefits with their PII and PHI, either directly or indirectly.

181. Defendants breached their obligations under their implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII and PHI in a manner that complies with applicable laws, regulations, and industry standards.

182. Defendants' breach of their obligations of its implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

183. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and Class members have suffered (and will continue to suffer), ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary

loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing medical information, bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

184. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class members sustained damages as alleged herein.

185. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

COUNT III
WISCONSIN CONFIDENTIALITY OF HEALTH RECORDS LAW,
WIS. STAT. §146.81, et seq.
(On behalf of the Plaintiffs and the Class Against 90 Degree Benefits, Inc.)

186. Plaintiffs repeat and reallege the forgoing allegations with the same force and effect as though fully set forth herein.

71. Wisconsin law regarding Confidentiality of Patient Health Care Records, WIS. STAT. §§146.81, *et seq*., states that:

> All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient."

WIS. STAT. §146.82(1).

72. Defendant 90 Degree Benefits, Inc. ("Defendant" for purposes of this Count) disclosed the private and protected medical information of Plaintiffs and Class members to unauthorized third parties without their knowledge, consent, or authorization.

73. Plaintiffs and Class Members provided their PII and PHI to a "health care provider" as defined by WIS. STAT. § 146.81(1).

74. Plaintiffs and Class Members are "patients," as defined by WIS. STAT. § 146.81(3) of Defendant's client-healthcare providers.

75. The stolen PII and PHI belonging to Plaintiffs and Class Members are "health care records" under WIS. STAT. § 146.81(4).

76. Defendant is a "covered entity" for purposes of WIS. STAT. § 146.82 and had a duty not to re-disclose any healthcare records in its possession regarding Plaintiffs and members of the Class. WIS. STAT. § 146.82.

77. Defendant re-disclosed healthcare care records pertaining to Plaintiffs and Class Members without their consent and for no other reason permitted by either WIS. STAT. § 146.82(5) or § 610.70, and therefore violated WIS. STAT. § 146.82.

78. Defendant violated WIS. STAT. §§146.81*, et seq*. through its willful and knowing failure to maintain adequate security measures, which allowed criminals to improperly access and compromise when it compromised, allowed access to, released, and disclosed patient health care records and PII and PHI without the informed consent or authorization of Plaintiffs and Class Members. Defendant did not and does not have express or implied consent to disclose, allow access to, or release the Plaintiffs' and Members' PII and PHI. To the contrary, Defendant expressly undertook a duty and obligation to Plaintiffs and Class Members.

79. Plaintiffs and Class Members were injured and have suffered damages as a result of Defendant's illegal disclosure and negligence release of their healthcare records in violation of WIS. STAT. § 146.82.

80. Defendant did not disclose to or warn the Plaintiffs and Class Members that their PII and PHI could be compromised, stolen, released, or disclosed to third parties without their consent as a result of Defendant's computer systems and software being outdated, easy to hack, inadequate, and insecure. Plaintiffs and Class Members did not know or expect, or have any reason to know or suspect, that Defendant's computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their PII and PHI to unauthorized disclosure.

81. WIS. STAT. §146.84(1)(b) states:

> Any person, including the state or any political subdivision of the state, who violates WIS. STAT. § 146.82 or § 146.83 in a manner that is knowing and willful shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $25,000 and costs and reasonable attorneys' fees.

82. WIS. STAT. §146.84(1)(bm) states:

> Any person, including the state or any political subdivision of the state, who negligently violates WIS. STAT. §146.82 or 146.83 shall be liable to ***any person injured*** as a result of the violation for actual damages to that person, ***exemplary damages*** of not more than $1,000 and costs and reasonable actual attorney fees. WIS. STAT. §146.84(1)(bm). [Emphasis added.]

83. WIS. STAT. §146.84(1)(c) states:

> An individual may bring an action to enjoin any violation of §§146.82 or 146.83 or to compel compliance with §§146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection.

84. Actual damages are not a prerequisite to liability for statutory or exemplary damages under WIS. STAT. §146.81. A simple comparison of other Wisconsin statues (*e.g.*, WIS. STAT. §134.97(3)(a) and (b), "Civil Liability; Disposal And Use" of records containing personal information), makes clear that the Wisconsin Legislature did not include an actual damages requirement in Wis. Stat. §146.84 when it explicitly did so in other privacy statutes. *See* WIS. STAT. §134.97(3)(a) and (b).

85. Similarly, the Wisconsin Legislature made it clear that the exemplary damages referred to WIS. STAT. §146.81 are not the same as punitive damages. Here, the plain language of another Wisconsin statue (WIS. STAT. §895.043(2), "Scope" of punitive damages), specifically and unequivocally excludes an award of "exemplary damages" under WIS. STAT. §§146.84(1)(b) and (bm) from the scope of "punitive damages" available under Section 895.043. In short, exemplary damages under WIS. STAT. §146.84(1)(b) and (bm) are not the same as either actual damages, or punitive damages; they are statutory damages available to persons who have been "injured" as a result of a negligent data breach like the one at issue here The plain, common dictionary definition of "injure" is, "**injured**; **injuring** play \'inj-riŋ, 'in-jə-\

> transitive verb
> **1a :** to do an injustice to **:** wrong
> **b :** to harm, impair, or tarnish the standing of
> • *injured* his reputation
> **c :** to give pain to
> • *injure* a person's pride
> **2a :** to inflict bodily hurt on
> **b :** to impair the soundness of
> • *injured* her health
> **c :** to inflict material damage or loss on."[32]

86. Plaintiffs and Class Members request that the Court issue declaratory relief declaring Defendant's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PII and PHI data between Defendant and third parties unlawful. The Plaintiffs and Class Members further request the Court enter an injunction requiring Defendant to cease the unlawful practices described herein,

[32] "Injure" Merriam Webster Online Dictionary (2021 ed.); *see also supra* note 5 (relying on Black's Online Law Dictionary (2d ed.) definition, stating an injury is "Any wrong or damage done to another, either in his person, rights, reputation, or property." *Parker v. Griswold*, 17 Conn.288, 42 Am. Dec. 739; *Woodruff v. North Bloomfield Gravel Mining Co.*, 18 Fed.753; *Hitch v. Edgecombe County Comm'rs*, 132 N. C. 573, 44 S.E. 30; *Macauley v. Tierney*, 19 R.I. 255, 33 Atl. 1, 37 L.R.A. 455, 61 Am. St. Rep. 770. In the civil law. A delict committed in contempt or outrage of anyone whereby his body, his dignity, or his reputation is maliciously injured. Voet, Com. Ad Pand. 47, t. 10, no. 1.

and enjoining Defendant from disclosing or using PII and PHI without first adequately securing or encrypting it.

87. Plaintiffs and Class Members request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing PII and PHI in their possession or the possession of third parties and provide it to the Plaintiffs and Class Members.

88. Plaintiffs and Class Members request that the Court enter an injunction ordering that Defendant:

a. engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct test, and audit Defendant's safeguards and procedures on a periodic basis;

b. audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

c. conduct regular checks and tests on its safeguards and procedures;

d. periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

e. meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps Defendants are taking to update its security technology to adequately secure and safeguard patient PII and PHI; and

f. identify to each Class Member in writing with reasonable specificity the PII and PHI of each such Class Member that was stolen in the Data Breach, including without limitation as required under WIS. STAT. §134.98(3)(c).

187. Plaintiffs and Class Members request the Court enter an Order pursuant to WIS. STAT. §146.84(1)(bm) awarding minimum statutory exemplary damages of $1,000 to each Plaintiff and each Class Member whose PII and PHI was compromised and stolen, as well as attorneys' fees and costs.

COUNT IV
WISCONSIN DECEPTIVE TRADE PRACTICES ACT,
WIS. STAT. §§100.18, *et seq.*,
(On behalf of the Plaintiffs and the Class)

188. Plaintiffs repeat and reallege the forgoing allegations with the same force and effect as though fully set forth herein.

189. The conduct of 90 Degree Benefits, Inc. ("Defendant" for purposes of this Count) violates Wisconsin's Deceptive Trade Practices Act, WIS. STAT. §100.18 (the "WDTPA"),[33] which provides that no,

> "firm, corporation or association,...with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

190. Defendant 90 Degree Benefits, Inc. is a "person, firm, corporation or association," as defined by WIS. STAT. § 100.18(1).

191. Plaintiffs and Class Members are members of "the public," as defined by WIS. STAT. § 100.18(1).

192. Plaintiffs and Class Members "suffered pecuniary loss because of a violation" of the WDTPA. WIS. STAT. §100.18(11)(b)(2).

[33] WIS. STAT. §110.18.

193. Defendant deliberately engaged in deceptive and unlawful practices, particularly after December 10, 2022, when Defendant asserted, represented, and stated on its website: "We recognize and respect your desire for privacy when it comes to your personal and health care affairs" and represented that "We maintain this information, as well as all web based transactions, according to our usual high, government regulated, security and confidentiality standards."[34] Among other things, Defendant continued to make this claim even though Defendants knew its network had been accessed via an earlier data breach in February 2022. Further, Defendant also continued to make this claim even after Defendants learned that its network had again been accessed in this Data Breach.

194. Defendants further violated the WDTPA by fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard PII and PHI from unauthorized access and misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, so as to safeguard PII and PHI from unauthorized access.

195. Defendants intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations, and therefore increase the sales and use of Defendants' goods and services.

[34] *See* https://90degreebenefits.com/privacy.php (last visited April 19, 2023).

196. Defendants' representations were material because they were likely to deceive reasonable consumers, including Plaintiffs and Class members, about the adequacy of Defendants' security measures and ability to protect the confidentiality of consumers' PII and PHI.

197. Defendants' representations were further material because they were likely to deceive reasonable consumers, including Plaintiffs and Class members, that their PII and PHI was not exposed and misled Plaintiffs and Class Members into believing they did not need to take actions to secure their PII and PHI exposed by Defendants.

198. Defendants knew or should have known that its computer systems and security practices and procedures were inadequate, and that risk of the Data Breaches and theft was high. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

199. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable loses of money or property, and monetary and non-monetary damages, including from fraud and identity theft, time and expense relating to monitoring their PII and PHI for fraudulent activity, an increased, imminent risk of fraud and identity theft; and loss of value of their PII and PHI.

200. Defendants had an ongoing duty to Plaintiffs and Class members to refrain from deceptive acts, practices, plans, and schemes under WIS. STAT § 100.18.

201. The Plaintiffs and the Class Members reasonably relied upon Defendants' deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. WIS. STAT. §§ 100.18(11)(b)(2).

COUNT V
Unjust Enrichment
(On behalf of the Plaintiffs and the Class)

202. Plaintiffs repeat and reallege the allegations of forgoing paragraphs with the same force and effect as though fully set forth herein.

203. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

204. Plaintiffs and Class members conferred a monetary benefit to Defendants when they provided their PII and PHI to receive Defendants' services.

205. Defendants knew that Plaintiffs and Class members conferred a monetary benefit to Defendants when they accepted and retained that benefit. Defendants profited from this monetary benefit, as the obtaining PII and PHI is an integral part of Defendants' business. Without Plaintiffs' and Class members' PII and PHI, Defendants would have dramatically diminished business and profits.

206. Defendants were supposed to use some of the monetary benefit provided to them from Plaintiffs and Class members to secure the PII and PHI belonging to Plaintiffs and Class members by paying for costs of adequate data management and security.

207. Defendants should not be permitted to retain any monetary benefit belonging to Plaintiffs and Class members because Defendants failed to implement necessary security measures to protect the PII and PHI of Plaintiff and Class members.

208. Defendants gained access to the Plaintiffs' and Class members' PII and PHI through inequitable means because Defendants failed to disclose that it used inadequate security measures.

209. Plaintiffs and Class members were unaware of the inadequate security measures and would not have provided their PII and PHI to Defendants had they known of the inadequate security measures.

210. To the extent that this cause of action is pled in the alternative to the others, Plaintiffs and Class members have no adequate remedy at law.

211. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiffs and Class members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

212. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, including,

but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

213. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds from the monetary benefit that they unjustly received from them.

COUNT VI
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

214. Plaintiffs repeat and reallege the allegations contained in foregoing paragraphs with the same force and effect as though fully set forth herein.

215. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

216. Defendants owed and owe a duty of care to the Plaintiffs and Class members that require they to adequately secure Plaintiff's and Class members' PII and PHI.

217. Defendants still possess the PII and PHI of the Plaintiffs and the Class members.

218. Defendants have not satisfied their contractual obligations and legal duties to the Plaintiffs and the Class members.

219. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to the Plaintiffs and the members of the Class. Further, the Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their PII and PHI and Defendants' failure to address the security failings that led to such exposure.

220. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

221. The Plaintiffs and the Class, therefore, seek a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants provide employee training regarding the dangers and risks inherent in using file-sharing websites;

e. Ordering that Defendants cease transmitting PII and PHI via file-sharing websites;

f. Ordering that Defendants cease storing PII and PHI on file-sharing websites;

g. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any PII and PHI not necessary for their provision of services;

h. Ordering that Defendants conduct regular database scanning and security checks; and

i. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs individually and on behalf of the Class, requests that the Court:

A. Certify this case as a class action on behalf of the Class defined above, appoint the Plaintiffs as the Class Representatives and appoint the undersigned counsel as Class counsel;

B. Award equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of the Plaintiffs and Class Members;

C. Award injunctive relief as requests by the Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiffs and Class Members;

vi. prohibiting Defendants from maintaining the PII and PHI of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to

promptly correct any problems or issues detected by such third-party security auditors

viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

xi. requiring Defendants to conduct regular database scanning and securing checks;

xii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment

D. Award the appropriate monetary relief to the Plaintiffs and Class members, including actual damages, nominal damages, statutory damages, consequential damages, treble damages, punitive damages, restitution, and all other such and further monetary relief as is just and proper;

E. Award Plaintiff and Class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

F. Award Plaintiff and Class members pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Dated: April 21, 2023

Respectfully Submitted,

/s/ John D. Blythin

Shpetim Ademi
John D. Blythin
ADEMI LLP
3620 East Layton Avenue
Cudahy, Wisconsin 53110
Tel.: (414) 482-8000
Fax: (414) 482-8001
sademi@ademilaw.com
jblythin@ademilaw.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

William B. Federman
FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560/(405) 239-2112 (facsimile)
wbf@federmanlaw.com

Attorneys for Plaintiffs

*application for admission forthcoming